

TRANSMITTAL OF APPEAL BRIEF (Large Entity)

Docket No.
00280552AA

In Re Application Of: R. Bolle, et al.

FEB 10 2005

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
09/489,908	1/24/00	V. Bali	30743	2623	6447

Invention: Improvements to a combined Fingerprint Acquisition and Control Device

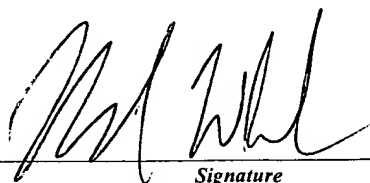
COMMISSIONER FOR PATENTS:

Transmitted herewith in triplicate is the Appeal Brief in this application, with respect to the Notice of Appeal filed on 12-15-04.

The fee for filing this Appeal Brief is: \$500.00

- ☐ A check in the amount of the fee is enclosed.
- ☐ The Director has already been authorized to charge fees in this application to a Deposit Account.
- ☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 50-0510 (IBM)
- ☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.


Signature

Dated: Feb. 10, 2005

Michael E. Whitham
Reg. No. 32,635

Whitham, Curtis & Christofferson, PC
11491 Sunset Hills Road - #340
Reston, VA 20190
Customer No. 30743

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

(Date)

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence

CC:



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re patent application of

Rudolf M. Bolle et al.

Serial No. 09/489,908

Group Art Unit 2623

Filed January 24, 2000

Examiner Vikkram Bali

For IMPROVEMENTS TO A COMBINED
FINGERPRINT ACQUISITION AND
CONTROL DEVICE

Commissioner for Patents

P.O. Box 1450

Alexandria, Virginia 22313-1450

APPELLANTS' BRIEF UNDER 37 C.F.R. § 1.192

This brief, which is filed herewith in triplicate, is in furtherance of the Notice of Appeal, filed January 10, 2005.

This brief contains these items under the following headings and in the order set forth below, as required under 37 C.F.R. § 1.192(c):

- I. REAL PARTY IN INTEREST
- II. RELATED APPEALS AND INTERFERENCES
- III. STATUS OF CLAIMS
- IV. STATUS OF AMENDMENTS
- V. SUMMARY OF INVENTION
- VI. ISSUES
- VII. GROUPING OF CLAIMS

YO999-270

02/14/2005 MBEYENE1 00000085 500510 09489908
01 FC:1402 500.00 DA

VIII. ARGUMENTS

☐ ARGUMENT VIIIA. REJECTIONS UNDER 35 U.S.C. §112, FIRST
PARAGRAPH

☐ ARGUMENT VIIIB. REJECTIONS UNDER 35 U.S.C. §112, SECOND
PARAGRAPH

☐ ARGUMENT VIIC. REJECTIONS UNDER 35 U.S.C. §102

☒ ARGUMENT VIID. REJECTIONS UNDER 35 U.S.C. §103

☐ ARGUMENT VIIE. REJECTION OTHER THAN 35 U.S.C. §§102, 103
AND 112

IX. APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

X. OTHER MATERIALS THAT APPELLANT CONSIDERS NECESSARY OR
DESIRABLE

I. REAL PARTY IN INTEREST

The real party in interest in the appeal is:

- ☐ the party named in the caption of this brief.
- ☒ the following party:

International Business Machines Corporation of Armonk, New York.

II. RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal:

☒ there are no such appeals or interferences.

☐ these are as follows:

III. STATUS OF CLAIMS

The status of the claims in this application is as follows:

A. Total number of claims in Application

The claims in the application are: Claims 1-4, 7, 9, 10-14, and 16-27, totaling 23 claims

B. Status of all the claims:

1. Claims cancelled: Claims 5, 6, 8, and 15
2. Claims withdrawn from consideration but not cancelled: None
3. Claims pending: Claims 1-4, 7, 9, 10-14, and 16-27
4. Claims allowed: None
5. Claims rejected: Claims 1-4, 7, 9, 10-14, and 16-27

C. Claims on Appeal.

The claims on appeal are: Claims 1-4, 7, 9, 10-14, and 16-27

IV. STATUS OF AMENDMENTS

The status of amendments filed subsequent to the final rejection is as follows:

There have been no amendments filed subsequent to the final rejection dated September 15, 2004.

V. SUMMARY OF INVENTION

The claimed invention concerns a method and systems combining the functionality of a computer pointing device with that of a fingerprint authentication system.

Most mobile computers currently incorporate some kind of pointing device, because pointing devices are essential for using widely-adopted operating systems and applications, including (without limitation) Microsoft Corporation's Windows, Apple Corporation's Mac OS, and many applications running under them. Beginning with the now-traditional mouse, a wide variety of pointing devices have been introduced, including trackballs, touchpads, and various mechanical pointers. Pointing devices other than the traditional mouse are more likely than the traditional mouse to be used with mobile computers, because mobile computers are often used in public places in which the large, flat space necessary for operating a traditional mouse is not available.

Not only are mobile computers likely to be used in places that are inconvenient for operating a traditional mouse, they are also likely to be used in unsecured areas where unauthorized persons might attempt to use or access the computer. Notwithstanding potential security risks, mobile computer users may view themselves as unable to avoid having confidential or proprietary information stored on their computers. Mobile telephones, personal digital assistants, and other portable electronic devices present similar security risks and, even if they do not contain confidential or proprietary information, may present risk of a financial loss if used by unauthorized persons.

Existing security systems for mobile computers and other portable electronic devices require active intervention by the user, such as by entering a password or locking and unlocking the device with a key. The perceived inconvenience of frequent password entry and of frequent locking and unlocking, in conjunction with users' fears of misplacing or forgetting a password or key, may result in failure to use existing security systems. Thus, difficulty-of-use issues may prevent existing security systems from being used adequately to safeguard mobile computers and other portable electronic devices.

In view of the desirability of a security system for mobile computers and other portable electronic devices, and in view of the widespread use of pointing devices on mobile computers and other portable electronic devices, one potentially attractive solution to the security problem is to employ a pointing device incorporating a fingerprint scanner. Powerful processors and algorithms, coupled with new, more compact fingerprint scanners, have made possible the automatic verification of fingerprints on small computer platforms, which typically have pointing devices built in anyway. Use of a combined pointing device and fingerprint scanner may allow for user authentication when the pointing device is touched, without requiring separate intervention by the user in forms such as entering a password or locking and unlocking the device with a key.

The claimed invention thus combines the functionality of a computer pointing device with a fingerprint authentication system. In the preferred embodiment, there is shown a computer 100, having as screen 110 and keyboard 120. Computer 100 is shown in Figure 1 with a combined fingerprint scanner and pointing device scanner 130 according to the claimed invention. Figure 2 shows a diagram of a fingerprint scanner surface 210 with an acquired fingerprint image 220. Fingerprint scanner surface 210 corresponds to the functional area of scanner 130. The portion of the surface area of scanner 130 which comprises scanner surface 210 depends upon the function characteristics of scanner 130, which may vary depending on the image acquisition method employed by scanner 130. By regularly scanning fingerprints acquired from the pointing device touch pad, fingerprint features may be extracted and compared to stored data on authorized users for passive authentication. The presently preferred embodiment of the claimed invention calculates a center-of-area or centroid 230 of fingerprint image 220. Centroid 230 has an associated two dimensional coordinate relative to fingerprint scanner surface 210, which in Figure 2 is represented as an x-coordinate 240 and a y-coordinate 250. The choice of coordinate systems is arbitrary, and may be chosen to facilitate computations related to the specific or general application of the device according to the claimed invention. This calculation is performed with each fingerprint image collected.

VI. ISSUES

The issues presented in this Appeal are:

- a) Whether Claims 1-9 and 11-13 are obvious over U.S. Patent No. 5,717,777 to Wong et al. in view of Japanese Patent No. 04158434 to Matsubashi.
- b) Whether Claim 10 is obvious over U.S. Patent No. 5,717,777 to Wong et al. in view of U.S. Patent No. 5,999,637 to Toyoda et al.
- c) Whether Claims 14-27 (it being understood that Claim 15 is canceled) are obvious over a combination of U.S. patent No. 5,717,777 to Wong et al. and either or both of Japanese Patent No. 04158434 to Matsubashi or U.S. Patent No. 5,999,637 to Toyoda et al.

VII. GROUPING OF CLAIMS

Claim Group 1. Claims disclosing a method for authenticating a user and for input of control information for an electronic device by acquiring at least two fingerprints through a scanner. (Claims 1-4, 7, and 9)

Claim Group 2. Claim disclosing a method for authentication and input control for an electronic device by comparing successive fingerprints taken through a scanner. (Claim 10)

Claim Group 3. Claims disclosing a method for authentication and input control for an electronic device using a reference image of a fingerprint. (Claims 11-13)

Claim Group 4. Claim disclosing an apparatus for authenticating a user and for input of pointing information for a computer using a fingerprint image acquisition scanner. (Claim 14)

Claim Group 5. Claims disclosing an apparatus for authentication and input control for a computer directing a user to follow through on any combination of a multiplicity of prompts. (Claims 16-17)

Claim Group 6. Claim disclosing an apparatus for authentication and input control for a computer wherein a motion of the finger tip is interpreted as a gesture for recognition by a gesture engine. (Claim 18)

Claim Group 7. Claims disclosing an apparatus for authentication and input control for a computer in which fingerprint data may also be used to identify at least one authorized user as a particular user. (Claims 19-21)

Claim Group 8. Claim disclosing an apparatus for imaging a fingerprint for input of control information for an electronic device. (Claim 22)

Claim Group 9. Claims disclosing an apparatus for authenticating a user and for input of pointing information for a computer using a multiplicity of fingerprint image acquisition scanners. (Claims 23-25)

Claim Group 10. Claims disclosing an apparatus for authentication and input control for a computer wherein a password may be entered by touching small fingerprint

scanners in a specific order. (Claims 26-27)

The claims of the above-mentioned groups do not stand or fall together. Reasons as to why the grouped claims are separately patentable are included in the arguments.

ARGUMENT VIII.A. REJECTIONS UNDER 35 U.S.C. §112, FIRST PARAGRAPH

There are no rejections under 35 U.S.C. §112, first paragraph.

ARGUMENT VIIIB. REJECTIONS UNDER 35 U.S.C. §112, SECOND PARAGRAPH

There are no rejections under 35 U.S.C. §112, second paragraph.

ARGUMENT VIIC. REJECTIONS UNDER 35 U.S.C. §102

There are no rejections under 35 U.S.C. §102.

ARGUMENT VIID. REJECTIONS UNDER 35 U.S.C. §103

Pursuant to a final rejection dated September 15, 2004 (the “Final Rejection”), Claims 1-4, 7, 9, 10-14, and 16-27 have been rejected under 35 U.S.C. § 103(a) as being obvious over various combinations of U.S. Patent No. 5,717,777 to Wong et al., Japanese Patent No. 04158434 to Matsubashi, and U.S. Patent No. 5,999,637 to Toyoda et al. In the Final Rejection, the Examiner for the first time requested confirmation that the subject matter of the various claims was commonly owned at the time of the invention. Appellants hereby provide that confirmation and state that there is no claim that was not commonly owned at the time of the invention.

In the substantive rejection of Claims 1-4, 7, 9, 10-14, and 16-27, the Examiner failed to consider the claimed invention and the references as a whole and has failed to determine obviousness by application of the standard of reasonable expectation of success. *Cf.* M.P.E.P. § 2141. For example, the references relied upon by the Examiner do not suggest use of a pointing device and fingerprint scanner controlling access to a computer or other electronic device by requiring at least two fingerprint images of a finger, which is a principal innovation of the claimed invention.

The Examiner argued in the Advisory Action dated December 7, 2004 (“Advisory Action”) that Wong et al. require at least two fingerprint images because “the first fingerprint is taken for enrolment [sic] and the second fingerprint is taken for authentication.” The Examiner’s own description of Wong et al., however, shows that the reference requires only one fingerprint image for access, since the first fingerprint image is taken for the purpose of enrollment and not access. The ability of the claimed invention to require more than a single live fingerprint scan for authentication may be useful for purposes such as preventing “replay attacks” using stored fingerprints to gain unauthorized access. (Specification, page 11, lines 12-18)

None of the references relied upon by the Examiner suggests that the fingerprint images and at least one contact parameter are used to authenticate a user and to control a computer or other electronic device, as in the claimed invention. Claim 1, for example,

discloses “acquiring through a scanner *at least two fingerprint images of a finger*” and “*computing image correlations between the acquired fingerprint images*” (emphasis added). This allows for “extracting from each said fingerprint image at least one contact parameter, *calculated by the step of computing image correlations*, the contact parameter being determined between image attributes in each said fingerprint image” (emphasis added).

Wong et al. do not describe the combination of a fingerprint scanner with a pointing device or any other feature of a mobile computer or other portable electronic device. While Matsubashi describes a pointing device combined with a fingerprint detection means, Matsubashi does not provide that the scanner acquire “at least two images of a finger.” (Claim 1, lines 3-4) (emphasis added) Furthermore, while Toyoda et al. describe an individual identification apparatus for selectively recording a reference pattern based on a correlation with comparative patterns, Toyoda et al. do not describe the combination of a fingerprint scanner with a pointing device or any other feature of a mobile computer or other portable electronic device.

Claim Group 1

Claim Group 1 (Claims 1-4, 7, and 9) is drawn to a method for authenticating a user and for input of control information for a computer or other electronic device by acquiring at least two fingerprints through a scanner. The claims of Claim Group 1 are distinct, and separately patentable, from the claims of other claim groups. Claim 1, which may be taken as exemplary of Claim Group 1, is drawn to method for authenticating a user and for input of control information for an electronic device comprising:

acquiring through a scanner incorporated into a pointing device at least two fingerprint images of a finger;

computing image correlations between a multiplicity of small regions of the acquired fingerprint images;

extracting from each said fingerprint image at least one contact parameter, calculated by the step of computing image correlations, the contact parameter

being determined between image attributes in each said fingerprint image; and
using said fingerprint images and said at least one contact parameter to
authenticate said user and to control said electronic device.

(Claim 1) Claims 2-3 add that the contact parameter may be rotation or translation.
Claim 4 adds that the method may further comprise pitch and roll rotations. Claims 7
and 9 add a step of determining the rate of change of some control parameter where a
rotation or translation of said finger relative to a reference position is used to determine
the rate of change of some control parameter of the computer, and that the reference
position may be the position at which contact with the scanner is first registered and that
the reference point may be reset every time a finger reestablishes contact with a scanner.

The Examiner found the limitation of Claim 1, concerning the acquisition through
a scanner of at least two fingerprint images of a finger, to be anticipated by a discussion
in the specification of Wong et al. The technique discussed by Wong et al., however, is
distinct from Claim 1, because only one fingerprint image (from which are taken “live
coordinate points” to be compared to “reference coordinate points”) is taken by Wong et
al. (Wong et al., column 1, line 64 through column 2, line 4) In Claim 1 of the claimed
invention, authentication may be based on more than a single live fingerprint scan, in
contrast to the one live fingerprint scan employed for authentication in the cited passage
from Wong et al. The ability of the claimed invention to require more than a single live
fingerprint scan for authentication may be useful for purposes such as preventing “replay
attacks” using stored fingerprints to gain unauthorized access. (Specification, page 11,
lines 12-18)

The Examiner has also found the limitation of Claim 1, “to authenticate said user
and to control said electronic device,” to be anticipated by a discussion in the
specification of Wong et al. Applicants, however, have not been able to find reference to
an “electronic device” either in the cited passage (Wong et al., column 2, lines 1-15) or
elsewhere in Wong et al. In addition, Wong et al. is directed to controlling “access to a
protected area” (Wong et al., column 1, lines 65-66) and does not appear to discuss or to
contemplate use of fingerprints to control access to computers or other electronic devices.

Because there is not any combination of Wong et al. and Matsubashi that would make obvious a method of authenticating a user and for input of control information that requires acquiring at least two fingerprint images of a finger and using the fingerprint images to authenticate a user and to control said electronic device, the claims of Group 1 (Claims 1-4, 7 and 9) would not be obvious. In addition, Claim 1 was amended prior to the Final Rejection to include the requirement of now-canceled Claim 6 that image correlations between a multiplicity of small regions of the acquired fingerprint imaged be computed. None of the references perform such computations on more than one image. In summary, neither reference uses two fingerprint images for authentication and device control.

The Examiner also erroneously found limitations of dependent Claims 2-4, relating to the use of “rotation,” “translation,” or “pitch and roll” in determining a contact parameter, to be anticipated by a discussion in the specification of Wong et al. However, where the reference discusses translation and rotation of a single live fingerprint image in order to compare it to a reference image (Wong et al., column 2, lines 10-14), Claims 2-4 derive from base Claim 1 the flexibility to permit authentication based on a comparison of two or more scanned fingerprint images to a reference fingerprint. In addition, there is no discussion of “pitch and roll” (Claim 4) in Wong et al.

The Examiner stated that Matsubashi describes a pointing device for display devices; the combination of Matsubashi with Wong et al. would not make the claims obvious. While Matsubashi describes a pointing device combined with a fingerprint detection means, Matsubashi does not provide that the scanner acquire “at least two images of a finger” (emphasis added) as in Claim 1, from which Claims 7 and 9 depend. As discussed above, the ability of the claimed invention to require more than a single live fingerprint scan for authentication may be useful for purposes such as preventing “replay attacks” using stored fingerprints to gain unauthorized access. (Specification, page 11, lines 12-18) Matsubashi does not suggest such a capability.

While Matsubashi describes a mouse that uses a fingerprint detector to assure that only authorized people perform certain data operations, Matsubashi uses a prior art

technique of enrollment, followed by comparison of the fingerprint acquired at preset intervals to the enrolled and stored fingerprint. This is quite different from the claimed invention, where two fingerprints and the contact parameter are used for security purposes.

Claim Group 2

Claim Group 2 (Claim 10) is drawn to a method for authentication and input control for an electronic device by comparing successive, possibly consecutive of a fingerprint taken through a scanner. Claim Group 2 is patentably distinct from Claim Group 1, because, among other things, Claim Group 2 describes a distinct method for using multiple images of a fingerprint taken from a single period of contact with a fingerprint scanner for authentication and input control.

The Examiner rejected Claim 10 as unpatentable over Wong et al. in view of Toyoda et al. Toyoda et al. describe an individual identification apparatus for selectively recording a reference pattern based on a correlation with comparative patterns. Like Wong et al. (and unlike the claimed invention), Toyoda et al. does not describe the combination of a fingerprint scanner with a pointing device or any other feature of a mobile computer or other portable electronic device. Toyoda et al. does not teach “comparing successive, and possibly consecutive, images taken from a single period of contact of said finger with said scanner” (Claim 10) but instead discusses the possibility of taking multiple sets of fingerprints “from each of ten fingers of the specific person” so that a “most appropriate” set of such fingerprints may be selected as a reference set based upon specific standards. (Toyoda et al., column 16, lines 1-16) As such, neither Wong et al. nor Toyoda et al. are utilizing at least two acquired images of a fingerprint for the purposes of authentication and of allowing control of an electronic device. All Toyoda et al. would add to Wong et al. is storing images of ten fingers, for example, for enrollment purposes. The combination would not result in or make obvious having successive images from a single period of contact to be used for authentication. Applicants thus respectfully submit that a combination of Wong et al. with Toyoda et al. would not result

in Claim 10 and that the claim is patentable over the references and should be allowed.

Claim Group 3

Claim Group 3 (Claims 11-13) is drawn to a method for authentication and input control for an electronic device using a reference image of a fingerprint. The claims of Claim Group 3 are distinct, and separately patentable, from the claims of other claim groups, in part because Claim Group 3 describes a distinct method for using a reference image of a fingerprint for authentication and control. Claim 11 requires that at least one of the fingerprint images to be used according to the claimed invention may be a reference image captured previously. Under Claim 12, the reference image may be labeled with known rotation information. Under Claim 13, a user may be prompted at an enrollment stage present a finger at known rotations in order to provide known rotation information.

The Examiner found limitations of dependent Claims 11-13 that “at least one of said fingerprint images is a reference image captured previously” to be anticipated by a passage from Wong et al. discussed in connection with Claim 1, above. (Wong et al., column 1, line 64 through column 2, line 4) However, Claims 11-13 derive from base Claim 1 the limitation that the claimed method is “for input of control information for an electronic device” (Claim 1). As discussed above in connection with Claim 1, Applicants could not find reference to an “electronic device” in Wong et al. In addition, Wong et al. is by its own terms directed to controlling “access to a protected area” (Wong et al., column 1, lines 65-66) and does not appear to discuss or to contemplate techniques to control access to electronic devices.

In view of the above, any combination of Wong et al. and Matsubashi would yield only the ability to compare one fingerprint against a stored image. No combination would require two fingerprints and a contact parameter for authentication

While Matsubashi describes a mouse that uses a fingerprint detector to assure that only authorized people perform certain data operations, Matsubashi uses a prior art technique of enrollment, followed by comparison of the fingerprint acquired at preset

intervals to the enrolled and stored fingerprint. This is quite different from the claimed invention, where two fingerprints and the contact parameter are used for security purposes.

Claim Group 4

Claim Group 4 (Claim 14) is drawn to a system for authenticating a user and for input of pointing information for a computer using a fingerprint image acquisition scanner. The claims of Claim Group 4 are distinct, and separately patentable, from the claims of other claim groups, in part because Claim Group 4 describes a distinct apparatus for authentication and control in which a fingerprint scanner may be able to capture successive images of a finger in motion. Claim 14 discloses a system for authentication and for input of pointing information for a computer, comprising:

- a fingerprint image acquisition scanner incorporated into a pointing device for acquiring at least two fingerprint images of a finger, wherein said scanner is able to capture successive images of a finger in motion on a surface of said scanner;

- computing means for computing image correlations between the acquired fingerprint images;

- an image processor for extracting from said fingerprint image at least one contact parameter calculated by said computing means, other than any optional authentication status data for said fingerprint image;

- verifying an acquisition of data in real time from a live user based on one or more variations in each of said contact parameters; and

- means for using said successive fingerprint images and said at least one contact parameter to control a pointing device and to authenticate said user.

(Claim 14)

The Examiner rejected Claim 14 on the basis that the claim is claiming subject matter combinations of rejected Claims 1-13 and should therefore be rejected for the same reasons.

The Final Rejection does not discuss any specific basis for rejecting Claim 14.

A combination Wong et al., Matsubashi, and Toyoda et al. would not result in any of the claims of the claimed invention, including but not limited to Claim 14. Wong et al. do not describe the combination of a fingerprint scanner with a pointing device or any other feature of a mobile computer or other portable electronic device as in Claim 14. The technique discussed by Wong et al. involves only one fingerprint image, from which are taken “live coordinate points” to be compared to “reference coordinate points.” (Wong et al., column 1, line 64 through column 2, line 4) Claims 14, by contrast, requires at least two fingerprint images, which is a principal innovating feature of the claimed invention. In addition, Wong et al. is by its own terms directed to controlling “access to a protected area” (Wong et al., column 1, lines 65-66) and does not appear to discuss or to contemplate techniques to control access to electronic devices.

As discussed above, the Examiner argued in the Advisory Action that Wong et al. require at least two fingerprint images because “the first fingerprint is taken for enrolment [sic] and the second fingerprint is taken for authentication.” The Examiner’s own words, however, show that Wong et al. require only one fingerprint image for access, since the first fingerprint image is taken for the purpose of enrollment and not access. As discussed above, requiring more than a single live fingerprint scan for authentication may be useful for purposes such as preventing “replay attacks” using stored fingerprints to gain unauthorized access. (Specification, page 11, lines 12-18)

While Matsubashi describes a pointing device combined with a fingerprint detection means, Matsubashi does not provide that the scanner acquire “*at least two fingerprint images of a finger*” (emphasis added) or that said scanner may be “able to capture successive images of a finger in motion on a surface of said scanner” as in Claim 14.

Toyoda et al. do not describe the combination of a fingerprint scanner with a pointing device or any other feature of a mobile computer or other portable electronic device, as in Claim 14. Toyoda et al. discuss the possibility of taking multiple sets of fingerprints “from each of ten fingers of the specific person” so that a “most appropriate”

set of such fingerprints may be selected as a reference set based upon specific standards. (Toyoda et al., column 16, lines 1-16) Toyoda et al. do not, however, suggest *inter alia* “means for using said successive fingerprint images and said at least one contact parameter to control a pointing device and to authenticate said user” or “verifying an acquisition of data in real time from a live user based on one or more variations in each of said contact parameters.” (Claim 14)

Even if Wong et al., Matsubashi, and Toyoda et al. could be combined, none of the references contemplates capturing “successive images of a finger in motion” as in required in Claim 14. It is this feature which separates Claim 14 from the other groups of inventions noted above, and if no prior reference utilizes capturing images of a finger in motion, no combination would make the claimed invention obvious. It is noted further that this feature assures that a live set of images is being taken and defeats a security attack where a fake fingerprint is employed.

Claim Group 5

Claim Group 5 (Claims 16-17) is drawn to a system for authentication and input control for a computer using a fingerprint image acquisition scanner further comprising means for directing a user to follow through on any combination of a multiplicity of prompts. The claims of Claim Group 5 are distinct, and separately patentable, from the claims of other claim groups, in part because Claim Group 5 describes a distinct apparatus for authentication and control in which a user response to a multiplicity of prompts for presenting a finger to fingerprint scanner in various positions. Claim 16 provides a system for identification and authorization in which a user may be directed to follow through on a multiplicity of prompts including, but not limited to: “change a position of, add pressure to contact or rotate said finger from which a fingerprint image is acquired and wherein said multiplicity of prompts are verified by the system to ensure that the data is being generated at the time of direction.” Claim 17 further provides “means for prompting the user to enact a sequence of finger actions previously registered by the user as a ‘password’ for the device.”

The Examiner rejected Claims 16-17 on the basis that the claims are claiming subject matter combinations of rejected Claims 1-13 and should therefore be rejected for the same reasons. The Final Rejection does not discuss any specific basis for rejecting Claims 16-17.

The features of Claims 16-17 do not appear to be discussed by any of Wong et al., Matsubashi, or Toyoda et al. Claims 16-17 depend from Claim 14, and, as noted above, none of the cited references captures successive images of a finger in motion; thus, no combination of references makes the claims of Group 5 obvious, especially as Claims 16-17 impose still further requirements on the authentication. Furthermore, Claims 1-13 do not disclose directing a user to follow through on any combination of a multiplicity of prompts as in Claims 16-17 (though Claim 13 discloses “prompting the user to present the finger at known rotations in an enrollment stage”). Thus, the Final Rejection does not provide a justification for not allowing Claims 16-17.

Claim Group 6

Claim Group 6 (Claim 18) is drawn to a system for authentication and input control for a computer using a fingerprint image acquisition scanner wherein a motion of the finger tip is interpreted as a gesture for recognition by a gesture engine. The claim of Claim Group 6 is distinct, and separately patentable, from the claims of other claim groups, in part because Claim Group 6 describes a distinct apparatus for authentication and input control in which the motion of the finger tip is interpreted as a gesture for recognition by a gesture engine.

The Examiner rejected Claim 18 on the basis that the claim is claiming subject matter combinations of rejected Claims 1-13 and should therefore be rejected for the same reasons. Thus, Final Rejection does not discuss any specific basis for rejecting Claim 18. Because none of the cited references contemplates a gesture for recognition, no combination of the references would make the claimed invention obvious.

Notwithstanding the rejection, the features of Claim 18 do not appear to be discussed by Wong et al., Matsubashi, or Toyoda et al. None of those references, for

example, appears to discuss a gesture engine, just as Claims 1-13 do not disclose a gesture engine. Thus, the Final Rejection does not provide a justification for not allowing Claim 18.

Claim Group 7

Claim Group 7 (Claims 19-21) is drawn to a system for authentication and input control for a computer using a fingerprint image acquisition scanner further comprising means by which fingerprint data used for authentication may also be used to identify at least one authorized user as a particular user. The claims of Claim Group 7 are distinct, and separately patentable, from the claims of other claim groups, in part because Claim Group 7 describes a distinct apparatus for authentication and input control in which fingerprint data may be to identify at least one authorized user as a particular user. Claim 19 describes such an apparatus further comprising:

- a feature extraction processor for extracting representative features from said fingerprint image;

- a memory for storing representative features of at least one authorized user; and

- a feature comparison processor for comparing said stored representative features with said extracted representative features, and generating authentication status data therefrom.

Claim 20 adds the feature “wherein an identity of a user is used to set customized features of the computer,” while Claim 21 adds the feature “where the identity of said user is used to set customized parameters of the pointing device.”

The Examiner rejected Claims 19-21 on the basis that the claim is claiming subject matter combinations of rejected Claims 1-13 and should therefore be rejected for the same reasons. The Final Rejection does not discuss any specific basis for rejecting Claims 19-21.

Notwithstanding the rejection, the features of Claims 19-21 do not appear to be discussed by Wong et al., Matsubashi, or Toyoda et al. None of those references, for example, discuss anything similar to the finger in motion requirement of base claim 14,

and none of the prior art references would make obvious a feature comparison operation, as contemplated by Group 7, Claims 19-21, in combination with a finger in motion requirement. Similarly, Claims 1-13 do not disclose identifying at least one authorized user as a particular user as in Claims 19-21. Thus, the Final Rejection does not provide a justification for not allowing Claims 19-21.

Claim Group 8

Claim Group 8 (Claim 22) is drawn to a system for imaging a fingerprint for input of control information for an electronic device. The claim of Claim Group 8 is distinct, and separately patentable, from the claims of other claim groups, in part because Claim 22 describes a distinct apparatus for authentication and control comprising:

- a fingerprint image acquisition scanner incorporated into a pointing device for acquiring at least two fingerprint images of a finger, wherein said scanner is able to capture successive images of a finger in motion on a surface of said scanner;

- computing means for computing image correlations between the acquired fingerprint images; and

- an image processor for extracting from said finger print image at least one contact parameter, representing the angle of the finger in relation to the scanner, where said angle is calculated by said computing means as correlations between image attributes of two or more images acquired from fingerprint image acquisition scanner,

- wherein said successive fingerprint images and said at least one contact parameter are used for control of said electronic device and for authentication of a user.

The Group 8 invention is in part similar to the Group 4 invention because of the requirement that the system be able to “capture successive images of a finger in motion” (emphasis added) and should be deemed unobvious over any combination of references for the same reasons discussed above. However, the Group 8 invention is also distinct from the Group 4 invention because of its requirements with respect to representing the

angle of the finger.

The Examiner rejected Claim 22 on the basis that the claim is claiming subject matter combinations of rejected Claims 1-13 and should therefore be rejected for the same reasons. The Final Rejection does not discuss any specific basis for rejecting Claim 22.

Notwithstanding the rejection, the features of Claim 22 do not appear to be discussed by Wong et al., Matsubashi, or Toyoda et al., just as Claims 1-13 do not disclose an apparatus for imaging successive images of a fingerprint. Matsubashi teaches a pointing device that detects a fingerprint pattern at preset time intervals but does not teach authentication or access control using a pointing device which takes successive fingerprints as in Claim 22. As discussed above in connection with Claim 10, which discloses a method that compares successive of a fingerprint taken through a scanner, Toyoda et al. discuss taking multiple sets of fingerprints “from each of ten fingers of the specific person” so that a “most appropriate” set of such fingerprints may be selected as a reference set based upon specific standards. (Toyoda et al., column 16, lines 1-16) Toyoda et al. do not suggest an apparatus for authentication and access control for an electronic device in which at least two successive fingerprint images of a finger are to be taken by the device’s built-in fingerprint scanner before user access can be obtained. Thus, the Final Rejection does not provide a justification for not allowing Claim 22.

Claim Group 9

Claim Group 9 (Claims 23-25) is drawn to a system for authenticating a user and for input of pointing information for a computer using a multiplicity of fingerprint image acquisition scanners. The claims of Claim Group 9 are distinct, and separately patentable, from the claims of other claim groups. Claim 23, which is the base claim of Claim Group 9 discloses an apparatus comprising:

a multiplicity of fingerprint image acquisition scanners incorporated into a pointing device providing a large input surface for acquiring successive fingerprint images of a finger;

computing means for computing image correlations between the successively acquired fingerprint images; and
an image processor for extracting from each said fingerprint image at least one contact parameter calculated by said computing means, other than any optional authentication status data for said fingerprint image; and
means for using said fingerprint images and said at least one contact parameter to authenticate said user and as input of pointing information for a computer.

(Claim 23) Claim 24 adds the limitation “where the scanner consists of a one-dimensional array of small fingerprint scanners,” while Claim 25 adds the limitation “where the scanner consists of a two-dimensional array of small fingerprint scanners.”

The Examiner rejected Claims 23-25 on the basis that the claims are claiming subject matter combinations of rejected Claims 1-13 and are therefore rejected for the same reasons. The Final Rejection does not discuss any specific basis for rejecting Claims 23-25.

Notwithstanding the rejection, the features of Claims 23-25 do not appear to be discussed by Wong et al., Matsubashi, or Toyoda et al. The Examiner has not identified any portion of any of the references as suggesting features of Claims 23-25, and Claims 1-13, to which the Examiner refers in rejecting Claims 23-25, contain no disclosure of an apparatus for imaging successive images of a fingerprint using a multiplicity of built-in fingerprint image acquisition scanners to provide a large input surface for acquiring successive fingerprint images to permit only authorized users to use an electronic device. Thus, the Final Rejection does not provide a justification for not allowing Claims 23-25.

Claim Group 10

Claim Group 10 (Claims 26-27) is drawn to a system for authentication and input control for a computer using a fingerprint image acquisition scanner further comprising means for inputting a password through a sequence of touching individual small

fingerprint scanners in a specific order. The claims of Claim Group 10 are distinct, and separately patentable, from the claims of other claim groups. Claim 26 discloses an apparatus in which inputting of a password is accomplished through a sequence of touching individual small fingerprint scanners in a specific order with the same finger. Claim 27 discloses an apparatus in which the password is a sequence or touching individual small fingerprint scanners in a specific order, with more than one finger being used in the sequence either serially or in parallel.

The Examiner rejected Claims 26-27 on the basis that the claims are claiming subject matter combinations of rejected Claims 1-13 and are therefore rejected for the same reasons. The Final Rejection does not discuss any specific basis for rejecting Claims 26-27.

Notwithstanding the rejection, the features of Claims 26-27 do not appear to be discussed by Wong et al., Matsubashi, or Toyoda et al. The Examiner has not identified any portion of any of the references as suggesting features of Claims 26-27, and Claims 1-13, to which the Examiner refers in rejecting Claims 26-27, contain no disclosure of inputting a password through a sequence of touching individual small fingerprint scanners in a specific order. Similarly, Claims 1-13 do not disclose inputting a password through a sequence of touching individual small fingerprint scanners in a specific order as in Claims 26-27. Thus, the Final Rejection does not provide a justification for not allowing Claims 26-27.

ARGUMENT VIII. REJECTION OTHER THAN 35 U.S.C. §§102, 103 AND 112

There is no rejection other than 35 U.S.C. §§102, 103, and 112 and no rejection other than the rejections under 35 U.S.C. § 103 discussed above.

IX. APPENDIX OF CLAIMS INVOLVED IN THE APPEAL (37 C.F.R. §1.192(c)(9))

The text of the claims involved in this Appeal are:

1. A method for authenticating a user and for input of control information for an electronic device, said method comprising:
 - acquiring through a scanner incorporated into a pointing device at least two fingerprint images of a finger;
 - computing image correlations between a multiplicity of small regions of the acquired fingerprint images;
 - extracting from each said fingerprint image at least one contact parameter, calculated by the step of computing image correlations, the contact parameter being determined between image attributes in each said fingerprint image; and
 - using said fingerprint images and said at least one contact parameter to authenticate said user and to control said electronic device.
2. A method as in claim 1, wherein said contact parameter is rotation.
3. A method as in claim 1, wherein said contact parameter is translation.
4. A method as in claim 1, further comprising calculating pitch and roll rotations.
5. (Canceled)
6. (Canceled)
7. A method as in claim 1, further comprising the step of determining the rate of change of some control parameter where a rotation or translation of said finger relative to a reference position is used to determine the rate of change of some control parameter of

the computer.

8. (Canceled)

9. A method as in claim 7, wherein said the reference position is the position at which contact with the scanner is first registered, further comprising the step of resetting the reference point every time the finger reestablishes contact with the scanner.

10. A method as in claim 1, further comprising the step of comparing successive, and possibly consecutive, images taken from a single period of contact of said finger with said scanner.

11. A method as in claim 1 wherein at least one of said fingerprint images is a reference image captured previously.

12. A method as in claim 11 wherein the reference image is labeled with known rotation information.

13. A method as in claim 12, further comprising the step of prompting the user to present the finger at known rotations in an enrollment stage to provide said known rotation information.

14. A system for authenticating a user and for input of pointing information for a computer, said system comprising:

a fingerprint image acquisition scanner incorporated into a pointing device for acquiring at least two fingerprint images of a finger, wherein said scanner is able to capture successive images of a finger in motion on a surface of said scanner;

computing means for computing image correlations between the acquired fingerprint images;

an image processor for extracting from said fingerprint image at least one contact parameter calculated by said computing means, other than any optional authentication status data for said fingerprint image;

verifying an acquisition of data in real time from a live user based on one or more variations in each of said contact parameters; and

means for using said successive fingerprint images and said at least one contact parameter to control a pointing device and to authenticate said user.

15. (Canceled)

16. A system as in claim 14, said system further comprising means for directing a user to follow through on any combination of a multiplicity of prompts including: change a position of, add pressure to contact or rotate said finger from which a fingerprint image is acquired and wherein said multiplicity of prompts are verified by the system to ensure that the data is being generated at the time of direction.

17. A system as in claim 14, said system further comprising means for prompting the user to enact a sequence of finger actions previously registered by the user as a "password" for the device.

18. A system as in claim 14 wherein a motion of the finger tip is interpreted as a gesture for recognition by a gesture engine.

19. The system of claim 14, further comprising:

a feature extraction processor for extracting representative features from said fingerprint image;

a memory for storing representative features of at least one authorized user; and

a feature comparison processor for comparing said stored representative features with said extracted representative features, and generating authentication status data

therefrom.

20. A system as in claim 19 wherein an identity of a user is used to set customized features of the computer.

21. A system as in claim 19 where the identity of said user is used to set customized parameters of the pointing device.

22. A system for imaging a fingerprint for input of control information for an electronic device, said system comprising:

a fingerprint image acquisition scanner incorporated into a pointing device for acquiring at least two fingerprint images of a finger, wherein said scanner is able to capture successive images of a finger in motion on a surface of said scanner;

computing means for computing image correlations between the acquired fingerprint images; and

an image processor for extracting from said finger print image at least one contact parameter, representing the angle of the finger in relation to the scanner, where said angle is calculated by said computing means as correlations between image attributes of two or more images acquired from fingerprint image acquisition scanner,

wherein said successive fingerprint images and said at least one contact parameter are used for control of said electronic device and for authentication of a user.

23. A system for authenticating a user and for input of pointing information for a computer, said system comprising:

a multiplicity of fingerprint image acquisition scanners incorporated into a pointing device providing a large input surface for acquiring successive fingerprint images of a finger;

computing means for computing image correlations between the successively acquired fingerprint images; and

an image processor for extracting from each said fingerprint image at least one contact parameter calculated by said computing means, other than any optional authentication status data for said fingerprint image; and

means for using said fingerprint images and said at least one contact parameter to authenticate said user and as input of pointing information for a computer.

24. A system as in claim 23, where the scanner consists of a one-dimensional array of small fingerprint scanners.

25. A system as in claim 23, where the scanner consists of a two-dimensional array of small fingerprint scanners.

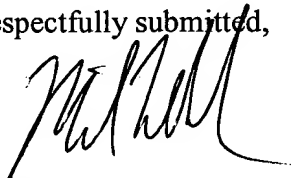
26. A system as in claim 17, where the "password" is a sequence of touching individual small fingerprint scanners in a specific order with the same finger.

27. A system as in claim 26, where the password is a sequence or touching individual small fingerprint scanners in a specific order, with more than one finger being used in the sequence either serially or in parallel.

X. OTHER MATERIALS THAT APPELLANT CONSIDERS NECESSARY OR DESIRABLE

There are no other materials considered necessary or desirable for consideration in this appeal.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Michael E. Whitham', written over the typed name.

Michael E. Whitham
Registration No.32,635

Whitham, Curtis & Christofferson, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA 20190
Tel. (703) 787-9400
Fax. (703) 787-7557
Customer No. 30743